

## SECURING ELECTRONIC TRANSACTIONS OVER PUBLIC NETWORKS

### Cross Reference to Related Applications

This application is related to pending Application Serial Number 09/017,169, filed February 2, 1998, entitled "Distributed Data Accessing Technique"; pending Application Serial Number 09/237,657, filed January 27, 1999, entitled "A Technique for Centrally Tracking Transactions in an Electronic Billing System"; pending Application Serial Number 09/301,068, filed April 28, 1999, entitled "An Electronic Bill Presentment Technique With Enhanced Biller Control"; pending Application Serial Number 09/414,731, filed October 8, 1999, entitled "Electronic Billing With Flexible Biller Controlled Electronic Bill Presentment"; pending Application Serial Number 09/387,764, filed September 1, 1999, entitled "Electronic Billing With Updateable Electronic Bill Summary"; pending Application Serial Number 09/208,998, and filed December 11, 1998, entitled "Technique for Conducting Secure Transactions Over a Network"; pending Application Serial Number 09/298,889, filed April 26, 1999, entitled "Electronic Bill Presentment and/or Payment Clearinghouse"; pending Application Serial Number 09/229,102, filed April 26, 1999, entitled "Cashless Transactions Without Credit Cards, Debit Cards or Checks".

### Technical Field

The present invention relates generally to electronic commerce and more particularly to securing electronic transactions made over public networks such as the Internet.

### Background Art

The Internet has had a profound affect on various aspects of everyday commerce. More and more individuals are utilizing the Internet to electronically perform tasks which were previously

performed in other ways. For example, electronic transactions are now commonplace on the Internet. Such transactions include electronic banking, electronic bill presentment, electronic bill payment and electronic purchasing.

5 As the use of the Internet for electronic commerce has developed, a model has emerged in which users often access other entities on the Internet through a trusted entity such as a financial institute. These entities through which access to other entities is made will hereinafter be referred to as "portals".

10 The portals are often supported by a service provider. The service provider, for example, may process electronic user requests, which are received by the portal, for information relating to a user's deposit account at a particular bank by electronically accessing information maintained by the applicable bank and processing that information so that it can be presented to the requesting user in a user friendly form.

15 Similarly, the service provider may also be the entity which responds to user requests received by the portal for billing information. For example, the service provider may receive summary bill information from numerous billers for numerous users and process this information such that the appropriate information can be presented in a user friendly manner in response to a request for bill information submitted by the user to the portal. However, if  
20 the user desires more detailed billing information, it is often preferable for the detailed bill information to be provided to the  
25 requesting user directly by the biller rather than by the service provider through the access portal.

30 Security of network communications relates to various aspects of protection. These include (i) secrecy, i.e. can someone other than the intended party view the data in transit?, (ii) immutability, i.e. how can one be assured that someone has not

altered the data in transit?, (iii) authentication, i.e. how can one ensure that each party in the conversation, e.g. session, is who it says it is?, (iv) authorization, i.e. is the authenticated party allowed to do what it is requesting to do?, and (v) non-  
5 repudiation, i.e. can a party repudiate its involvement, e.g. its actions?.

Secrecy is generally provided by encrypting data. For example, encrypted HTML, i.e. HTML/HTTPS (SSL), is used to insure that unintended parties can not see the information as it travels  
10 across the network, e.g. the Internet. However, this does not prevent the various transit points, e.g. the service provider and the portal, from viewing data that travels over the network. Thus, for example, a URL to a payor's detailed bill information could be misappropriated at a transit point or from the payor's terminal, e.g. from the payor's browser history, and could then later be used to access the payor's detailed bill information.

Like secrecy, immutability is also generally provided by encrypting the data. Typically, due to the nature of the algorithms, encryption which provides good secrecy also provides good immutability. For example, HTML/HTTPS is used to insure immutability as the data bits are travelling across the network. That is, even if one were to improperly access data off a network router, or at a transit point, it would be virtually impossible to read the misappropriated data; however, the data still could be  
25 altered. Thus, for example, an account number associated with the payor's detailed bill information could be misappropriated at a transit point and mangled. If this were to occur, the biller would have no way of confirming that a payor account number, originally sent by the portal to the payor and then sent by the payor to the  
30 biller with the request for detailed bill information, has not been misappropriated and mangled before being received by the biller.

Figure 1 is a somewhat simplified network diagram indicating various channels which may be established between network entities to provide electronic bill presentment services. As shown in Figure 1, the network includes users A-C which are represented on a network by network devices 105A-105C. The network devices 105A-105C could, for example be any device capable of communicating over the network, such as a personal computer, palm computer, set top box etc. Billers A-C are also represented on the network by network devices 110A-110C, typically although not necessarily high power workstations, mini-computers or mainframe computers, often referred to as servers. The network also includes an access portal 115 and a service provider 120.

Users A-C access services available on the network by establishing channels 125A-125C with the access portal 115. The access portal is linked to the service provider 120 by channel 130. The service provider in turn is linked to the billers A-C by channels 135A-135C.

For example, the channels 125A-125C may be Internet channels which are established through an Internet access provider, such as America Online (not shown), using a browser, such as browsers currently available from Microsoft Corporation and Netscape Corporation. Accordingly, the communications between the user devices 105A-105C and the access portal 115 are typically encrypted HTML communication, i.e. HTML/HTTPS.

Communications between the access portal 115 and the service provider 120 typically will follow a protocol such as IFX, or OFX etc., which may better ensure the security of the communications whether the link is via a private network or a public network such as the Internet. Similarly, communications between the service provider 120 and the biller network devices 110A-110C will also typically follow an established protocol and be transmitted via

channels 135A-135C which are provided on a private or public network.

If detailed bill information is desired by a user, further communications channels must be established between the requesting user and the appropriate biller. Accordingly, if user A desires detailed billing information relating to the bills of billers A-C communication links 140A-140C will be required as shown in Figure 1. These communication links will typically be established via the Internet using an Internet browser and accordingly carry encrypted HTML communications. It will be recognized that channels similar to channels 140A-140C could be established between user devices 105B and 105C and biller devices 110A-110C to communicate detailed bill information from billers A-C to users B and C.

Each of the users A-C will typically be known to different network entities by different identifiers. For example, as shown in Figure 2, each of the users A-C are known to each of the billers A-C by the user's name, e.g. A, B or C, the applicable user's address, e.g. ZA, ZB or ZC, and a unique account number, e.g. AA-CC which each biller associates with each user.

The access portal 115 will typically know each of the users A-C by a unique user name, e.g. A'-C' and a unique password, e.g. PA-PC. Alternatively, users may be known to the access portal 115 by a digital certificate, e.g. a digital signature, although this is relatively uncommon today.

The user name and password or digital certificate are often referred to as the user's credentials and are used by the access portal 115 to authenticate the user. The access portal 115 then vouches for authenticated users to other network entities. Should a particular user also have a transactional relationship with the access portal, for example if the access portal is a user's financial institute or stock brokerage firm, the user will also

typically be known to the access portal by additional information similar to that shown in the biller columns of Figure 2.

Figure 3A depicts typical communications between and functions of various network entities in providing bill summary information to a requesting user. As shown, network device 105A, representing user A, implements a browser 305, typically stored on a local memory, to communicate its credentials via an encrypted HTML communication over the Internet channel 125A to the access portal 115. The access portal 115 processes the credentials to authenticate user A, as indicated by reference numeral 310. Portal 115 then provides a response, as represented by the communicated authentication message, to network device 105A either granting or denying access based on whether or not user A has been successfully authenticated by the processing of the credentials. If access is granted, user A, operating network device 105A, may now request bill summary information from the access portal 115 via the channel 125A.

Having authenticated user A, the access portal 115 transmits the request for bill summary information via a protocol over channel 130 to the service provider 120. In response to the request, the service provider 120 retrieves the bill summary information and applicable universal resource locators (URL's) 315 from, for example, a local memory. The bill summary information and URL's 315 are typically provided by the billers via protocol or batch transmissions over channels 135A-135C to the server 120 off-line, i.e. in non-real time, with respect to the user request for the bill summary information.

The bill summary information and URL's are provided over channel 130 from the service provider 120 to the access portal 115. The access portal 115 then directs the bill summary and associated URL's to the user Internet device 105A via the Internet channel

125A in an encrypted HTML message.

Accordingly, bill summary information and URL's flow via a protocol from the biller to the service provider and from the service provider to the access portal. The bill summary information is only provided by the access portal to the user after authentication of the user. Further, the bill summary information and associated URL's for a particular user are provided to the access portal for transmission to the requesting user only if the access portal can vouch for the user to the service provider based upon its authentication of the user.

The URL's associated with the bill summary information represent the addresses to the bill detail information stored on the network 100 for the transmitted summarized bill information.

The bill detail information of billers A-C may be respectively stored, for example, on the memories 320A-320C. It should be recognized that, as described in the above-referenced related applications, the bill detail information could also or alternatively be stored at the service provider 120 or at another network site controlled, for example, by a bill aggregator. In any event, the URL's to the bill detail information are passed, along with the bill summary information, from the service provider 120 to the access portal 115 and from there to the user network device 105A. Typically each URL is embedded as a hyperlink in the applicable bill summary information presentation which will appear on a display included in the network device 105A.

A typical display is shown in Figure 4. Figure 4 depicts a display 400 of network device 105A which is used to present the requested bill summary information for user A. As shown, the presentation includes the names of billers A-C in display areas 405A-405C, the applicable bill amounts XA-XC billed by each of the billers A-C to user A in display areas 410A-410C, and a view bill

request area associated with each of the billers A-C in display areas 415A-415C which can be clicked on using a mouse or other input device to activate the applicable hyperlink URL HA-HC, identified with reference numerals 420A-420C, to establish a link to the bill detail information underlying the bill summary information being presented. The applicable bill may also be paid directly from the bill summary presentation by clicking on the appropriate pay bill area 425A-425C.

As shown in Figure 3B, by clicking on view bill area 415A and thereby activating the URL HA identified with reference numeral 420A in Figure 4, the user network device 105A is linked via an encrypted HTML Internet channel 140A to the biller address, i.e. URL address HA, at which the detailed bill information of the biller A for user A is stored. The detailed bill information is then provided via the channel 140A to the user A network device 105A without either the request or the provided detailed bill information flowing through the service provider 120 or access portal 115.

It should be understood that, if the bill detail information were stored at the service provider 120 or an aggregator (not shown), the hyperlink would link directly to an address at the aggregator or service provider network site at which the requested detailed bill information is maintained. In any event, the access portal 115 does not vouch for user A to biller A, the aggregator, or the service provider 120 in connection with the bill detail request and the bill detail information is communicated to the user A from biller A, the aggregator or the service provider 120 without flowing through the access portal 115.

This lack of authentication by the access portal 115 in connection with the bill detail request from user A is sometimes referred to as "the problem of transitive authentication". To



address this problem it has been proposed to implement an OFX protocol (i.e. Open Financial Exchange Specification 1.51 dated November 23, 1995, www.OFX.net) such that the creator of the bill detail information, e.g. the biller, aggregator or service provider etc., create a somewhat extended URL.

As shown in Figure 5A, in the proposed implementation of OFX 1.51, the somewhat extended URL 500 includes a network address 505 for the bill detail information, a bill identification (ID) 510 which identifies the particular bill being requested, and a user account number 515 which the biller associates with the applicable user. As indicated in Figure 5A, the bill ID and user account number are typically encrypted, but may instead be hashed.

Figure 5B presents a more realistic depiction of the somewhat extended URL 500 of Figure 5A for a typical Internet address prior to encrypting or hashing the bill ID 510 and user account number 515. More particularly, Figure 5B depicts the somewhat extended URL 500' with the network address 505', the bill ID 510' and the account number 515'.

The somewhat extended URL 500' provides the recipient of the request for detailed bill information, e.g. the biller, bill aggregator or service provider, with sufficient information to identify the particular bill based on the bill ID 510' and to verify the user account number based on account number 515', prior to allowing access to the detailed bill information stored at address 505'. However, the recipient has no way of verifying that the request has actually been made by the appropriate user, for example user A as shown in Figure 3B. Furthermore, there is no way for the recipient to know whether the somewhat extended URL originally transmitted by the access portal 115 has been tampered with and, for example, includes modified e.g. mangled, address, bill ID and/or user account number information.

For example, it is impossible for the recipient to know if the somewhat extended URL has been improperly copied from the user's browser either by operation of the user's network device on which the somewhat extended URL may be stored, by hacking into the information stored on the user's network device by the browser, or by installing coding, such as a JAVA applet, which automatically transmits information stored on the user's network device without user's knowledge to a network device under the control of others. It is also impossible for the recipient to know if the encrypted data has been altered. Hence, the proposed implementation of OFX 1.51 cannot ensure the integrity of the somewhat extended URL or serve as an aid in authenticating to the recipient that the requester is who he/she says he/she is.

Accordingly, a need remains for a technique to address the problem of transitive authentication.

#### Objectives of the Invention

Accordingly, it is an objective of the present invention to address the problem of transitive authentication.

It is another objective of the present invention to provide a technique which protects the integrity of the URL's which are used to access private information over a network.

It is also an objective of the present invention to provide a technique which allows a request recipient to authenticate the requesting party.

Additional objects, advantages, novel features of the present invention will become apparent to those skilled in the art from this disclosure, including the following detailed description, as well as by practice of the invention. While the invention is described below with reference to a preferred embodiment(s), it should be understood that the invention is not limited thereto.

Those of ordinary skill in the art having access to the teachings herein will recognize additional implementations, modifications, and embodiments, as well as other fields of use, which are within the scope of the invention as disclosed and claimed herein and with  
5 respect to which the invention could be of significant utility.

### Summary Disclosure of the Invention

In accordance with the invention a networked system for accessing information includes a first network station, such as a network server or other network device, which represents a first  
10 network entity, for example a biller. A second network station, which could be another network server or some other network device, represents a second network entity, such as an access portal, and controls access to the network by a third network entity. The first station controls access to information, such as detailed bill or other information, stored on a network for the third network  
15 entity, such as a customer of the biller. The first station encrypts a first component message, sometimes simply referred to as a first component of an aggregate message, with a first crypto-key associated with the first network entity, e.g. the biller.

The first crypto-key could be a symmetric crypto-key which is known only to the first network entity. Alternatively, the first crypto-key could be a non-symmetric crypto-key, such as a public crypto-key of a joint private-public crypto-key pair associated with the first network entity. In any event, beneficially the  
20 first network station encrypts the first component message off-line, i.e. in non-real time. That is, preferable the first network station encrypts the first component message at a time other than the time of a request, such as a request for bill summary information, which will be responded to by transmitting the  
25 encrypted first component message. The first component message preferably includes identity information associated with the third  
30

network entity, and integrity information which corresponds to the identity information. The identity information advantageously includes an identification of information stored on the network, such as a bill ID and/or an account number. The integrity  
5 information could, for example, include a hash of the identity information. In a typical implementation, the first network station combines the encrypted first component message with a network address for the stored information.

The integrity information provides enhanced immutability, by  
10 ensuring that the first network entity can verify that a returned first component message has not been mangled or otherwise altered. For example, if the first component message includes a bill ID and payor account number which is returned to the biller by the payor with the request for detailed bill information, the biller can use the integrity information to verify that the returned bill ID and account information are the same bill ID and account number included in the first component message.

The second network station encrypts a second component  
15 message with a second crypto-key and combines the encrypted first and the encrypted second component messages. The combined messages are then transmitted over the network, which could for example be the Internet. It would be recognized by those skilled in the art that the second crypto-key could, if desired, also be applied to the encrypted first component message at the time of encrypting the  
20 second component message.

The second crypto-key could be a non-symmetric crypto-key.

The non-symmetric crypto key might, for example, be a private crypto-key of a joint private-public crypto-key pair associated with the second network entity. Alternatively, the second crypto-  
25 key could be a symmetric crypto-key known also to the first network entity. In any event, preferably the second network station encrypts the second component message and combines the encrypted

first and the encrypted second component messages on-line, i.e. in real time. That is, the second network station beneficially encrypts the second component message and combines it with the encrypted first component message at the time of a request, e.g. a bill summary request, which will be responded to by transmitting the combine component messages.

The second component message preferably includes voucher information which indicates that the second network entity has authenticated the third network entity. The voucher information enhances authentication by allowing the second network entity to vouch for the third network entity to the first network entity. The voucher information can be used to authenticate who the third network entity is and, if desired, the third network entity's relationship with the second network entity. This allows, for example, a portal to confirm to a biller that the payor requesting detailed bill information is who he/she says he/she is and that the payor has a relationship with the portal.

Advantageously, the second component message also includes a timestamp corresponding to a time at which the combined messages are transmitted by the second network station. The timestamp enhances secrecy by preventing a misappropriated combined messages from later, i.e. beyond some designated time period after the time indicated by the timestamp, being used to access the information, such as detailed bill information. The timestamp also enhances non-repudiation, since it can be used by the first network entity to confirm that the combined messages were recently transmitted by the second network entity to the third network entity. Thus, for example, the timestamp can be used by a biller to confirm that a request for detailed bill information was received promptly after the associated bill summary information had been provided by a portal to the applicable payor.

A third network station, such as a personal computer or other network device, represents the third network entity and receives the transmitted combined messages, or what might also be referred to as an aggregate message formed of combined component messages.

5 The third station further transmits the received combined messages over the network in order to obtain access to the stored information. In this regard, the first network station receives the further transmitted combined messages, and decrypts the encrypted first and the encrypted second component messages  
10 contained therein. The first network station then controls access by the third network station to the stored information based on the decrypted first and second component messages. For example, if the first station is unable to successfully decrypt either of the component messages, access would typically be denied. If the decrypted first component message is associated with an entity different than the entity being vouched for in the second component message access would also be denied. If the timestamp indicates that a threshold time period has expired since the second network station transmitted the combined message, access may be denied.

15  
20 In accordance with other aspects of the invention, a fourth network station, such as another server or network device, represents a fourth network entity, for example a service provider. The fourth network device encrypts a third component message with a third crypto-key and initially combines the encrypted first and  
25 third component messages. The fourth network station then transmits the initially combined messages over the network.

30 The third crypto-key could be a non-symmetric crypto-key, which, for example, might be a private crypto-key of a joint private-public crypto-key pair associated with the fourth network entity. Alternatively, the third crypto-key could be a symmetric crypto-key known also to the first network entity. In any event, preferably the fourth network station encrypts the third component

message and combines the encrypted first and the encrypted third component messages on-line, i.e. in real time. That is, the fourth network station advantageously encrypts the third component message and combines it with the first component message at the time of a request, e.g. a bill summary request, which will be responded to by transmitting the combined messages. The public crypto-keys associated with the second and fourth network entities, could be distributed by either one of these entities, or by each of these entities, or by some other network entity.

The third component message preferably includes relationship information which indicates that the identity and integrity information was received by the fourth network entity from the first network entity and transmitted by the fourth network entity to the second network entity.

The second network station receives the transmitted initially combined messages, and combines the encrypted first and the encrypted third component messages contained therein with the encrypted second component message to create the above described combined messages. Hence, the first network station can decrypt the encrypted third component message and also use this message to control access by the third network station to the stored information. For example, if the information in the third component message is inconsistent with that in the second component message, access will be denied.

It should be understood that as used herein, the network could be made up of multiple sub-networks, some of which could be public while others are private. For example, in a bill presentment and payment implementation, the first and third network stations and the second and third network stations might communicate over the Internet, while the fourth network station communicates with the first network station via the Internet or some other network, and

with the second network station over the Internet or some still further network.

In accordance with other aspects of the invention, an electronic message has a first component created by a first network entity and encrypted with a first crypto-key, associated with the first network entity, such that the encrypted first component can be decrypted by only the first entity. The message also includes a second component created by a second network entity, and encrypted with a second crypto-key, such that the encrypted second component can also be decrypted by the first network entity. In some implementations, the message may advantageously additionally include a third component created by a third network entity and encrypted with a third crypto-key, associated with the third network entity, such that the encrypted third component can be decrypted by the first network entity.

According to further aspects of the invention an electronic message, includes a first component encrypted with only a symmetric crypto-key and a second component, different than the first component, encrypted with only a non-symmetric crypto-key. In certain implementations the symmetric crypto-key is associated with a first entity, and may only be known to the first entity, while the non-symmetric crypto-key is associated with a second entity.

The non-symmetric crypto-key may beneficially be a private crypto-key of a joint private-public crypto-key pair associated with the second entity.

In accordance with still other aspects of the invention, an extended network universal resource locator (URL) which is particularly suitable for Internet commerce includes a first component having a network address at which stored information can be accessed on a network. The extended URL also includes a second component having identity information associated with a first network entity and an integrity value corresponding to the identity



information. The second component is encrypted with a first crypto-key of a second network entity. The extended URL additionally includes a third component having relationship information indicating that the encrypted second component was received by a third network entity from the second network entity and transmitted by the third network entity to a fourth network entity. The third component is encrypted with a second crypto-key of the third network entity. The extended URL further includes a fourth component having voucher information indicating that the fourth network entity has authenticated the first network entity and that transmission of the extended URL by the fourth network entity to the first network entity occurred at a particular time. The fourth component is encrypted with a third crypto-key of the fourth network entity.

For example, if the extended universal resource locator is implemented in connection with electronic bill presentment via the Internet, the stored information could be detailed bill information. The network address would be an Internet URL. The identity information could include an identification of the stored information, e.g. detailed bill information and an account number associated with the first network entity. Preferably, the integrity value is a hash of the identity information and the transmission time information is a timestamp.

In such an implementation, the second network entity might be a biller or other entity which controls access to the stored information, such as the detailed bill information. The third network entity, might be a service provider, such as CheckFree Corporation, which controls access to other information, such as summary bill information, which is transmitted with the extended network universal resource locator by the fourth network entity to the first network entity, which might be the customer. The fourth

network entity might an access portal which controls access by the first network entity to other entities on the network.

### Brief Description of Drawings

Figure 1 depicts a conventional bill presentment network.

• 5        Figure 2 depicts the user identification information conventionally available to the access portal and the billers of Figure 1.

10        Figure 3A depicts a typical message flows between a user, the access portal, the service provider and a biller to request and present bill summary information via the Figure 1 network.

Figure 3B depicts a typical message flows between and a user and a biller to request and present detailed bill information via the Figure 1 network.

15        Figure 4 depicts a conventional presentation of bill summary information to the user shown in Figure 3A.

Figure 5A depicts a conventional URL for use by the user shown in Figure 3B in requesting detailed bill information.

Figure 5B is a more realistic depiction of the URL of Figure 5A.

20        Figure 6 depicts message flows between a user, the access portal, the service provider and a biller to request and present bill summary information via the Figure 1 network in accordance with the present invention.

25        Figure 7 depicts a portion of the collaboratively manufactured extended URL for use in requesting detailed bill information as shown in Figure 6, in accordance with the present invention.

30        Figure 8 depicts another portion of the collaboratively manufactured extended URL for use in requesting detailed bill information as shown in Figure 6, in accordance with the present invention.

Figure 9 depicts a combination of summary bill information and the portions of the collaboratively manufactured extended URL shown in Figures 7 and 8, in accordance with the present invention.

Figure 10 depicts still another portion of the collaboratively manufactured extended URL for use in requesting detailed bill information as shown in Figure 6, in accordance with the present invention.

Figure 11 depicts a combination of summary bill information and the collaboratively manufactured extended URL, in accordance with the present invention.

#### Best Mode for Carrying out the Invention

Although the present invention will now be described in the context of bill presentment, it should be recognized that the invention has wide applicability and can be easily adapted for use in obtaining virtually any type of private information by a user directly from the custodian of that information. For example, the present invention may have significant application in web banking, web brokerage, web mortgaging, request for credit reports, etc. without requiring the user to sign-on with other than its access portal during the session, even though the user will access the information directly from an entity other than the access portal during the session.

Figure 6 depicts typical communications between and functions of various network entities in providing bill summary information to a requesting user with a collaboratively manufactured extended URL. As shown, and previously described with reference to Figure 3A, network device 105A representing user A implements a browser 305 to communicate its credentials via an encrypted HTML communication over the Internet channel 125A to the access portal 115. The access portal 115 processes the credentials to authenticate user A as indicated by reference numeral 310, and

provides a response, as represented by the communicated authentication message, to network device 105A either granting or denying access based on whether or not User A has been successfully authenticated by the processing of the credentials. If access is granted, user A, operating network device 105A, can now request bill summary information from the access portal 115 via the channel 125A.

Having authenticated user A, the access portal 115 transmits the request via a protocol over channel 130 to the service provider 120. As described above with reference to Figure 5, in accordance with OFX 1.5 the URL 500 conventionally provided to the service provider 120 from the biller includes a network address (NA) for the bill detail information 505, a bill ID (BID) 510 which identifies a particular bill being requested and the account number (AN) 515 which the biller associates with the applicable user.

As shown in Figure 7, in accordance with the present invention, the biller performs a hash computation, H, on the network address (NA) 505 for the bill detail information, the bill ID (BID) 510 which identifies a particular bill being requested and the account number (AN) 515 which the biller associates with the applicable user to form an integrity value (IV) 520 as follows:

$$H[NA + BID + AN] \quad (1)$$

The bill ID 510, user account number 515 and the integrity value 520 are then encrypted using a symmetric encryption key E to form an encrypted message as follows:

$$NA + E [BID+AN+IV] \quad (2)$$

It should be understood that, if desired, the encryption could be performed using the biller's non-symmetric public key of a joint

private/public key pair, in lieu of the symmetric key E. In either case, the encryption and integrity value ensure the integrity of the base data, i.e. the bill ID 510 and the user account number 515, and the identification of the applicable user, in this case user A. The encrypted integrity value provides enhanced protection against altering of the information which will be returned to the biller by the payor with the request for detailed bill information. Hence, the biller can be confident that the exact bill ID, account information and user identification sent to the user is returned with user's the request for detailed bill information.

As also shown in Figure 7, in accordance with the present invention, the encrypted bill ID 510, user account number 515 and integrity value 520 are also signed using a digital certificate S(1), preferably supplied by the service provider 120 but which could alternatively be supplied by a separate certificate authority, to form an encrypted, signed extended URL message 700 to the detailed bill information as follows:

$$NA + [E [BID+AN+IV]]S(1) \quad (3)$$

The bill summary information (BSI) and the encrypted, signed extended URL message 700 are provided by each biller A-C, preferably via a secure protocol or batch communication over channels 135A-135C, to the service provider 120 in a message 315' as the following:

$$BSI + NA + [E [BID+AN+IV]]S(1) \quad (4)$$

Hence, responsive to the request from the access portal 115, the service provider 120 can retrieve, for example from a local memory, the applicable message(s) 315'.

Continuing with the collaborative manufacture of the extended

URL which will ultimately be returned to the user requesting the bill information, the service provider 120 creates, either prior to, i.e., off-line, or at the time of the request for the bill summary information, i.e., on-line, an encrypted, signed relationship certification (RC) 800, as shown in Figure 8. The relationship certificate includes a certification 810 that the service provider 120 received each of the applicable encrypted, signed extended URL messages 700 from the applicable biller A-C and a certification 820 that the service provider 120 is delivering the applicable encrypted, signed extended URL messages 700 to the access portal 115. The access portal 115 may, for example under the OFX protocol, be identified to the service provider 120 in the request for bill summary information received by the service provider 120 from the access portal 115.

As shown in Figure 8, the relationship certificate is encrypted, using the service provider's 120 non-symmetric private key, PKSP(2), of its joint private key PKSP (2)/public key PUBKSP(2) pair, and digitally signed using the service provider's 120 digital certificate S(2). Thus the encrypted, signed relationship certificate will take the form of a message such as the following:

[[RC]PKSP(2)]S(2) (5)

The encrypted relationship certificate will ensure that the commercial parties, i.e., the service provider 120 and the access portal 115, are identified in the extended URL.

As shown in Figure 9, the bill summary information 910 and a further extended URL message, including the encrypted, signed extended URL message 700 and the encrypted, signed relationship certificate 800, are transmitted over channel 130 from the service provider 120 to the access portal 115 in a further extended message

900 in the following form:

BSI + NA + [E[BID+AN+IV]]S(1) + [[RC]PKSP(2)]S(2) (6)

It should be recognized that the message 900 may be created and stored by the service provider 120 prior to receiving a request for the bill summary information or created in response to the receipt of such a request.

After receipt of message 900, the access portal 115 may, if desired verify that message 900 is from the service provider 120 and intended for the access portal 115 by applying the public key PUBKSP(2) of service provider 120 to the encrypted relationship certificate as follows:

[[RC]PKSP(2)]PUBSP(2) (7)

The access portal 115 continues the collaborative manufacture of the still further extended URL which will ultimately be returned to the user requesting the bill information. In this regard, the access portal 115 creates a voucher (V) 1005, depicted in Figure 10, which identifies the access portal 115 and indicates that the access portal 115 has authenticated the user, in this case user A. The access portal 115 then encrypts, using the access portal's 115 non-symmetric private key, PKAP(3), of its joint private key PKAP(3)/public key PUBKAP(3) pair, and signs, using a digital certificate, S(3), provided by the service provider 120 or some other certificate authority, the voucher (V) 1005 and a time stamp (TS) 1010 to form an encrypted, signed voucher record (VR) 1000 as follows:

[[V + TS]PKAP(3)]S(3) (8)

The encrypted, signed voucher will ensure that it can be verified that the applicable user is known to the access portal 115, and the encrypted, signed timestamp will ensure that the bill detail request has only a limited lifetime.

5 More particularly, the voucher enhances authentication. That is, the voucher, which will be transmitted by the portal to the user with the bill summary information and by the user to the biller with the request for detailed bill information as will be described further below, serves as the portal's confirmation to the  
10 biller that the payor is in fact who he/she says he/she is and that the payor has a relationship with the portal.

The timestamp enhances secrecy and non-repudiation by preventing the network address 505 in the collaboratively manufacture extended URL 1150 from being used to access the user's detailed bill information after a short timeout, i.e. threshold, period, e.g. 30 minutes from the transmission of the extended URL 1150 by the portal. Although not foolproof, since the timestamp prevents a misappropriated network address 505 from being used to access detailed bill information after a relatively short period of time, the likelihood that a request to access detailed bill information from some misappropriating party will be granted, is significantly reduced. Furthermore, because the timestamp evidences that the bill summary information associated with the now requested detailed bill information was recently, i.e. within the  
20 timeout period, transmitted to the user by the portal, it is more difficult for the user to repudiate its receipt of the bill summary information and/or of its request for access to the detailed bill information.

The bill summary information and the still further extended  
30 URL 1150, including the encrypted, signed extended URL message 700, the encrypted, signed relationship certification 800, and the encrypted, signed voucher record 1000, are transmitted as the



$$5 \quad \text{BSI} + \text{NA} + [\text{E}[\text{BID} + \text{AN} + \text{IV}]]\text{S}(1) + [[\text{RC}]\text{PKSP}(2)]\text{S}(2) + \quad (9)$$

$$[\text{VR}]\text{PKAP}(3)]\text{S}(3)$$

Accordingly, the access portal 115 directs to the user network  
10 device 105A, via the channel 125A in an encrypted HTML message, a  
message 1100 having a very rich, collaboratively manufactured  
extended URL 1150 including:

- 30

With the collaboratively manufactured extended URL 1150 of message 1100, as shown in Figure 11, substituted for the URL 500 shown in Figure 5, the display 400 of Internet device 105A presents, as shown in Figure 4, the requested bill summary for user A. The presented bill summary includes a view bill request area associated with each of the billers A-C in display areas 415A-C. The view bill request area can be clicked on using a mouse or other input device to activate the applicable collaboratively manufactured extended URL 1150 forwarded in message 1100 to hyperlink to the bill detail information underlying the applicable bill summary information being presented, as previously described with reference to Figure 3B. Thus, by clicking on view bill area 415A and thereby activating the collaboratively manufactured extended URL 1150 to the bill detail for biller A's bill, the user network device 105A is linked via an encrypted HTML channel 140A to the address at which the detailed bill information of the biller A for user A is stored as described with reference to Figure 3B.

However, before the detailed bill information is provided via the channel 140A to the user A network device 105 A, the biller checks the signature S(1) on the encrypted bill ID 510, user account number 515 and integrity value 520, and decrypts, using the corresponding symmetric decryption key D or the billers non-symmetric private key, as applicable, the bill ID 510, user account number 515 and integrity value 520 as follows:

$$D[BID+AN+IV] \quad (10)$$

The biller verifies the decrypted bill ID 510 and user account number 515 and, using the integrity value 520, also verifies that this information was the same information which it originally forwarded to the service provider 120.

Further, the biller checks the signature and then decrypts the

encrypted relationship certificate using the public key, PUBKSP(2), of the service provider 120 as follows:

[[RC]PKSP(2)]PUBKSP(2) (11)

The biller, using the relationship certificate, verifies that the service provider 120 received the bill ID 510, user account number 515 and integrity value 520 from the applicable biller and forwarded this information to the access portal 115.

Further still, the biller checks the signature and then decrypts the encrypted voucher record using the public key, PUBKAP(3) of the access portal 115 as follows:

[[VR]PKAP(3)]PUBKAP(3) (12)

The biller, using the voucher record, verifies that the access portal 115 identified in the relationship statement of the service provider 120 vouches for the applicable user, and that, based on the time stamp, the time period within which the request for detailed bill information has been received is within a designated threshold, preferably two to five minutes.

Hence, not only is bill summary information transmitted via a secure protocol from the biller to the service provider and from the service provider to the access portal, but the bill summary information is not transmitted until after the applicable user is authenticated by the access portal. Further, the bill summary information for a particular user is provided to the access portal for transmission to the requesting user only if the access portal 115 can vouch for the user to the service provider 120 based upon its authentication of the user. Moreover, the collaboratively manufactured extended URL 1150 provides the request recipient, e.g. the biller, bill aggregator or service provider etc., information

necessary to identify the particular bill and verify the user account number prior to allowing access to the detailed bill information.

5 Additionally, using the above described technique, the recipient now has a way of verifying that the request has actually been made by the appropriate user, for example user A as shown in Figure 6. More particularly, the collaboratively manufactured extended URL 1150 provides the recipient with the ability to verify that the information originally transmitted by the access portal  
10 has not been tampered with and hence, reflects the correct network address, bill ID and user account number information. Further, the collaboratively manufactured extended URL 1150 makes it possible for the recipient to determine if the information has been improperly copied from user A's browser. Hence, by collaborative manufacture the integrity of the information and authenticity of the requesting party can be ensured.

As described above, the present invention addresses the problem of transitive authentication. Further, the present invention provides a technique which protects the integrity of the URL's which are used to access private information over a network.  
15 Additionally, the present invention provides a technique which allows a URL to be utilized by a request recipient to authenticate the requesting party.

It will also be recognized by those skilled in the art that,  
25 while the invention has been described above in terms of one or more preferred embodiments, it is not limited thereto. Various features and aspects of the above described invention may be used individually or jointly. Further, although the invention has been described in the context of its implementation in a particular environment and for particular purposes, e.g. creating extended  
30 URL's, those skilled in the art will recognize that its usefulness is not limited thereto and that the present invention can be

beneficially utilized in any number of environments and implementations. Accordingly, the claims set forth below should be construed in view of the full breadth and spirit of the invention as disclosed herein.

2025-01-27 10:00:00